In the Specification:

Amend the Abstract as follows:

A system and method for providing trusted browser verification services ~~service are disclosed~~. In a preferred embodiment, these services are provided within the context of a four-corner trust model comprising a subscribing customer and a relying customer, engaged in an on-line transaction. The subscribing and relying customers are preferably customers of first and second financial institutions, respectively, that issue to them hardware tokens for their respective private keys and digital certificates. The buyer is preferably provided with a Web browser to conduct electronic transactions. A distinct-trusted verifier or other entity ensures in a verifiable manner that the browser used by the subscribing customer does not contain any code that is not trusted by verifying the digital signatures on each running browser component of the subscribing customer's browser and ensuring that the signature was applied by an entity that is authorized to certify the trustworthiness of the component. ~~In addition, the trusted verifier may compare a hash of the running browser components to known-good hashes for those components.~~

Replace the paragraph starting on page 4, line 32, with the following:

In a preferred embodiment, the system of FIG. 1 also comprises one or more trusted verifiers 201 shown in FIG. 1 as part of participants 102, 104. As discussed below, the trusted verifier 201 ensures the trustworthiness of Web browsers used by customers 106, 108. The trustworthiness of a customer's Web browser may be compromised by viruses or other means. The trusted verifier 201 allows relying parties to determine the verifiable trustworthiness of a browser.

Replace the paragraph starting on page 11, line 14, with the following:

In step 710, trusted verifier 201 retrieves from trusted component database 232 the identities of those entities authorized to certify the trustworthiness of each browser component in the browser

status request. It then determines whether the entity that executed the digital signature on each signed component is authorized to do so. For example, if the component is the Netscape ~~Communicator~~™ COMMUNICATOR™ browser, ~~Netscape~~™ NETSCAPE™ (i.e., the entity that created the component) may be designated as a trusted entity to certify the integrity of this component. Similarly, if the component was a ~~Microsoft~~™ MICROSOFT™ applet downloaded by the user, ~~Microsoft~~™ MICROSOFT™ might be designated a trusted entity to certify the integrity of this component. Alternatively or in addition, issuing participant 102 may be designated a trusted entity authorized to certify browser components running on its' customers' computers (e.g., subscribing customer 106). Alternatively or in addition, another system entity, such as trusted verifier 201, may be designated a trusted entity to certify the integrity of one or more browser components.